# Las amenazas a la privacidad, el mayor problema de seguridad informática en 2013

ESET presenta el resumen de las principales amenazas del año. Los especialistas del Laboratorio de Investigación de ESET Latinoamérica dan a conocer el resumen de los hechos más relevantes en materia de amenazas informáticas durante el 2013. Según los investigadores, los temas destacados rondaron en torno a la aparición de nuevos códigos maliciosos, vulnerabilidades críticas y violaciones a la privacidad.
A continuación se transcribe el informe de amenazas que más destacaron a lo largo del año, según ESET:

•Privacidad en Internet: El caso de Edward Snowden ha contribuido al aumento de la preocupación de los usuarios con respecto a su privacidad en Internet. El tema ha estado en el centro de la discusión durante todo el 2013 y seguramente siga así durante el año siguiente.

Otro tipo de ataque a la privacidad de los usuarios en Internet es aquel en el que los cibercriminales se aprovechan de vulnerabilidades o errores de diseño en los servicios más utilizados, para la recopilación de información confidencial. Como ejemplos pueden citarse los casos de Facebook, en el cual 6 millones de usuarios vieron su información expuesta, y Twitter con 250.000 usuarios comprometidos.

•Secuestro de información: Durante el 2013, han resurgido los códigos maliciosos de tipo Ransomware en diversas formas. Este tipo de malware tiene la capacidad de cifrar archivos en la computadora del usuario infectado, ya sean de texto, planillas de cálculo, fotos o videos. Luego se solicita el pago de un

rescate para poder acceder nuevamente a la información personal. En Latinoamérica se detectó el caso de Multi Locker, un troyano controlado mediante un Centro de Comando y Control (C&C). De acuerdo a las estadísticas obtenidas, México es el país de Latinoamérica más afectado por este código malicioso. Además, tuvo relevancia el caso de Nymaim, que variaba el precio solicitado en cada país, y que pedía 150 dólares para liberar las máquinas afectadas en México.

•El gusano de Skype: Rodpicom fue uno de los códigos maliciosos más destacados en América Latina. Utilizando técnicas de Ingeniería Social, este gusano se propagó enviando mensajes a los contactos de Skype y Gtalk de un usuario infectado. Al hacer clic en el enlace descargaba una supuesta imagen en la computadora, que realmente consistía en un archivo ejecutable malicioso. Tuvo un gran impacto, afectando a más de 300 mil usuarios a unas pocas horas desde el inicio de la campaña.

•Servidores vulnerables y troyanos bancarios: El Laboratorio de Investigación de ESET Latinoamérica detectó un código malicioso que se propagaba a través de una campaña de spam. El mismo instalaba un plugin de Google Chrome para interceptar todas las páginas web que navegaba la potencial víctima, en búsqueda de sitios web bancarios pertenecientes a entidades financieras de Brasil. Además, el código malicioso utilizaba un servidor gubernamental legítimo de ese país (que contenía un error de diseño) para el envío de la información. Se trató de una amenaza avanzada con la potencialidad de afectar a muchos usuarios brasileños.

•Vulnerabilidades: Durante este año se conocieron muchas vulnerabilidades para diversas aplicaciones. A lo largo de todo el año pudo observarse cómo Java seguía sumando vulnerabilidades críticas, muchas de las cuales permitían la ejecución de código en forma remota.

•Otras amenazas: Por un lado, el caso de Cdorked, un backdoor

que afectó a más de 400 servidores web de Apache, Lighttpd y nginx, muchos de ellos de sitios populares. Luego, una falsa aplicación de Adobe Flash que se propagó por Google Play y que realmente era un tipo de malware que buscaba recopilar información sensible del usuario. En cuanto al malware de 64 bits, éste ha visto un crecimiento durante este año; en la región, México y Perú son los países de Latinoamérica más afectados por malware de 64 bits. Por último, durante el 2013 se ha observado cómo las botnets Tor son actualmente una tendencia en crecimiento.

Fuente: Diario TI